## Zes antivirusprogramma's getest

# Hou beestjes buiten!

**Wie dacht dat het zo langzamerhand bergaf gaat met de virussen, komt helaas bedrogen uit. Gewoon rondsurfen op internet kan je al zo'n gedrocht aan je been lappen, maar het gebeurt ook steeds vaker via een onschuldige e-mail. Antivirussoftware moet je tegen dat soort vandalenstreken beschermen. En wij zijn er om te kijken of die bescherming ook wel doet wat de reclame belooft.**

Windows is zo lek als een zeef. Dat lezen we geregeld in allerlei artikelen. Het heeft bugs die je systeem onstabiel maken, het heeft gaten in zijn beveiliging die hackers toegang geven tot je systeem en virussen hebben ook al niet veel moeite om je pc te besmetten. Auteurs van virussen richten zich natuurlijk juist op Windows, want dat is nu eenmaal het meest gebruikte besturingssysteem. Je hoort dan wel eens roepen dat je geen last hebt van dingen als het Lirva- of Yaha-virus en allerlei ander vies spul dat via e-mail naar je toekomt, als je geen Windows draait. Dat is natuurlijk wel zo, maar dan kan je ook niet al die Windowssoftware die op de markt is, draaien. En laten we wel wezen: als je een winkel binnenloopt, voor welk besturingssysteem vind je dan software in de rekken? Juist ja: voor Windows. Hoewel je leven met een ander besturingssysteem erg aangenaam kan zijn omdat het niet crasht, geen hackers aan boord laat en geen virusinfecties te vrezen heeft, kan het een heel groot probleem zijn om er software voor te vinden. Voor de meeste mensen komt het er dus op neer dat Windows een vast gegeven is en zij niet echt een andere keuze hebben. Er is dus een markt voor software die al die gaten, lekken en kwetsbaarheden van Windows dicht. Antivirussoftware bijvoorbeeld. Helaas loopt zulke software per definitie achter op de prestaties van de virusmakers. Zo moet een nieuw virus eerst pc's besmet hebben voordat de antivirusspecialisten aan het werk kunnen gaan en er een remedie voor bedenken. Virusauteurs ontdekken steeds nieuwe dingen en verzinnen steeds nieuwe trucjes. Het valt dan ook op, dat de allernieuwste virussen steeds meer schade aanrichten. In het slechtste geval moet je zelfs een nieuw moederbord kopen. En ook bedrijven worden niet gespaard: er zijn hopen virussen die complete servers of tenminste allerlei diensten daarop platleggen en zelfs gespuis dat Windowssystemen zo beschadigt dat alleen formatteren nog helpt.

## Preventie!

Laten we wel wezen: detectie is niet genoeg. Een scanner vindt namelijk alleen maar virussen die al bekend zijn. Als er dan een virus op je systeem komt dat nog niet bekend is, kan dat vrijelijk zijn gang gaan en heel wat schade aanrichten. Ga er dus van uit dat een scanner nooit alle virussen kan vinden en dat er dus altijd wel door de mazen van het net glippen. Dat blijkt ook uit onze detectietest: van de bijna negentienduizend virussen die we voorlegden aan de scanners bleken zelfs de allerbeste er een dikke vijfhonderd niet te vinden. En het ging hier over bekende virussen! Reden te over dus om zeker geen blind vertrouwen te hebben in antivirussoftware. Een scanner helpt je om bekende virussen te detecteren, maar je hebt dus nood aan maatregelen die een virus verhinderen zijn vuile werk te doen. We plaatsen al die maatregelen onder de noemer preventie. Goede preventie zorgt ervoor dat een onbekend virus je systeem niet kan infecteren, of zich althans niet kan voortplanten. Zelf moet je natuurlijk ook een paar dingen doen en laten. Voer dus programma's die je van anderen krijgt nooit zomaar uit en lees documenten ook nooit zomaar in. Eerst even een virusscan uitvoeren is de boodschap. Alles wat je van het internet haalt of wat via e-mail al dan niet ongevraagd naar je toe wordt gestuurd is natuurlijk per definitie verdacht. Klik NOOIT op aanhangsels! ActiveX en *VB-scripts* zijn erg goede manieren om virussen in je systeem binnen te smokkelen. Uitschakelen dus of tenminste software draaien die dergelijke toepassingen in de gaten kan houden.

## Paniek zaaien

Geregeld verschijnen allerlei berichten over nieuwe virussen. Hoe weet je nu wat daarvan echt is en wat gewoon een paniekzaaierig verzinsel is? Er bestaan goede webpagina's hierover. Je kan een blik werpen op de Computer Virus Myths Homepage [ **www.vmyths.com** ] en dan zie je meteen of een bericht een verzinsel is. Informatie over de laatste nieuwe echte virussen is te vinden op de websites van de meeste antivirussoftwareproducenten. Een andere mogelijkheid is de WildList [ **www.wildlist.org** ]: dat is een lijst van virussen die werkelijk pc's geïnfecteerd hebben en gerapporteerd werden door virushulporganisaties (meestal afdelingen van antivirussoftware-producenten) wereldwijd.

## ANTIVIRUSPROGRAMMA'S EN BEVEILIGINGSSUITES

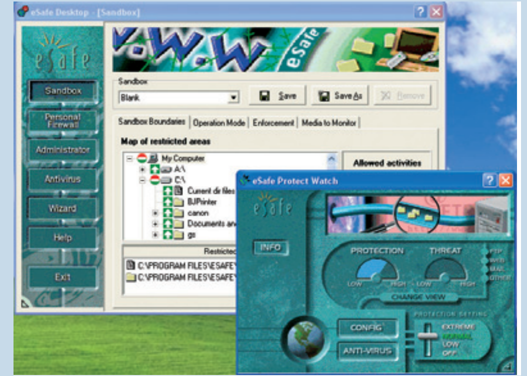
De meeste producenten van antivirussoftware geven je tegenwoordig de keuze tussen een hele waslijst aan producten. We scharen dat allemaal onder de noemer 'beveiligingssoftware'. Antivirussoftware is daar slechts één klasse van. Andere soorten beveiligingssoftware zijn persoonlijke firewalls, e-mailrommelfilters (spam- en junkfilters), software voor ouderlijk toezicht ('parental control software') en privacybeschermers (ad- en junkware-verwijderaars). Je kan natuurlijk van al deze soorten beveiligingssoftware een pakket kopen, maar dan ben je een pak geld kwijt. Gelukkig brengen de producenten ook zogenaamde beveiligingssuites op de markt: dan worden een aantal van deze programma's gebundeld in één pakket. Dat is veel goedkoper. Zowat alle producenten hebben dit. Als je dus meerdere beveiligingspakketten van eenzelfde producent wil hebben, kijk je beter uit naar de beveiligingssuite van die producent. Als je natuurlijk de beste beveiligingspakketten wil kiezen tussen het aanbod van meerdere producenten, dan heb je niks aan hun beveiligingssuite en zijn het de losse deelpakketten die je moet hebben. Er is één situatie waarin je toch de voorkeur kan geven aan een suite boven een los product. In sommige gevallen voert de producent immers een promotie en dan kan het voorkomen dat een complete suite goedkoper is dan één los onderdeel ervan. Dan profiteer je er natuurlijk van om de suite te kopen, ook al ben je niks met meerdere of zelfs alle andere programma's in deze suite, buiten degene die je wou hebben.

## VAKTAAL

**VB-script:** Een scripttaal van Microsoft waarmee men functies van Windows activeert en regelt. VB-script is gebaseerd op Visual Basic.

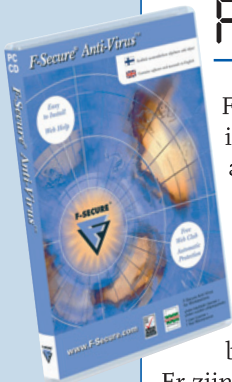
# eSafe Desktop



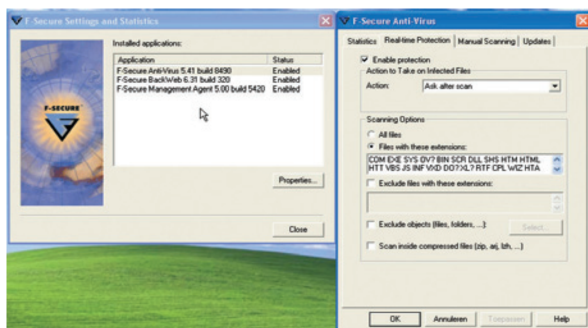


Dit van oorsprong Israëlische product werkt als enige met een zandbaksysteem. eSafe Desktop houdt vrij letterlijk álles in de gaten. Heel aardig is dat het binnengehaalde programma's in feite niet blokkeert, maar onder strikt toezicht (in een zogenaamde software-zandbak) uitvoert om te kijken of ze zich als vandalen gedragen. Zo ja, dan grijpt eSafe Desktop in voordat zulke software of applicaties wat kunnen doen. Dit beperkt je mogelijkheden als gebruiker niet (in tegenstelling tot andere soorten van preventiesoftware) en vangt toch alle mogelijke vandalenstreken op. Een probleem is wel de juiste afstelling van deze preventie. Als je de beveiliging hoog zet en niet aanpast, krijg je namelijk om de haverklap waarschuwingsvenstertjes en dat is niet echt leuk om werken. Een goed evenwicht vinden tussen beveiliging en werkbaarheid is dus de boodschap. De eigenlijke scanner blijkt echter vrij zwak en detecteert nogal slecht. Schoonmaken van besmette bestanden is zelfs vrijwel onbestaande. Als je die zandbak aan hebt staan, is dat echter niet eens zo belangrijk. Alle door de scanner onontdekte virussen werden namelijk keurig afgeblokt toen ze probeerden ons testsysteem te infiltreren. Sommige gebruikers beschouwen zelfs cookies als een vandalenstreek en ook daar kan je eSafe Desktop voor configureren. Verder kan je zelf uitgebreid opgeven welke data op je systeem zeker nooit het internet op mogen en je al dan niet laten waarschuwen als iets of iemand dat toch probeert. Tenslotte zit er ook nog een persoonlijke *firewall* à la ZoneAlarm in. Als je écht veilig wil surfen, kan je wat ons betreft nauwelijks buiten zo'n gecombineerd systeem met zandbak en firewall. Vroeger kon je eSafe gratis downloaden en gebruiken, maar dat is niet langer zo. Het product wordt nu beheerd door een Engelse firma genaamd LCSG, voor de oorspronkelijke maker Aladdin Knowledge Systems en die wil geld zien. Je kan het nog wel downloaden, maar dat is een evaluatieversie en na dertig dagen is het afdokken of kinkloppen. En het is niet goedkoop!

# F-Secure AntiVirus



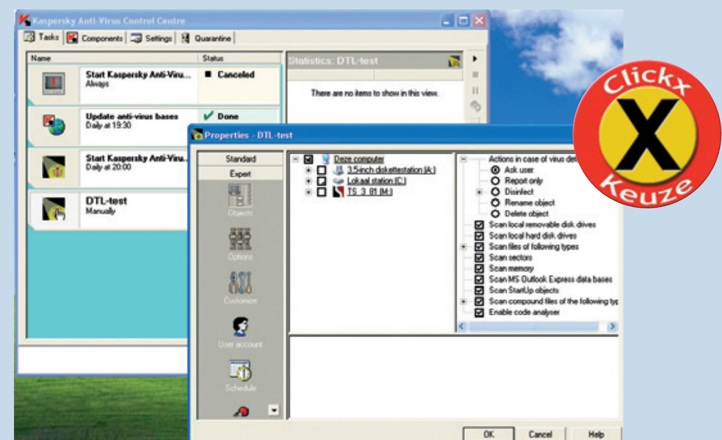
F-Secure AntiVirus (FSAV) is uit Finland afkomstig. Het is minstens zo oud als de McAfee virusscanner. Net zoals bij de andere software in deze test draait er bij wijze van preventie een permanente achtergrondtaak in Windows die je systeem in de gaten houdt. Je kan de eigenlijke detector manueel of geautomatiseerd starten. Voor dat laatste is er een op takenbeheer gesteunde interface. Hierbij maak je uit te voeren taken aan, waarbij je aangeeft wat er moet gebeuren, wanneer en hoe. Er zijn al een aantal voorbeeldtaken aanwezig die je kan gebruiken als model, maar je mag ook volledig van de grond af een taak opbouwen. Updates haal je met een druk op de knop van het internet, maar het gaat niet zo makkelijk als bij sommige andere pakketten. Overigens kan je bij de installatie kiezen tussen een alleenstaande software-installatie of een netwerkinstallatie waarbij je de andere FSAV-pakketten centraal kan beheren. Interessant: bij inspectie van de updates bleken die afkomstig te zijn van het Kaspersky Lab in Rusland en daar komt ook het pakket hiernaast vandaan. FSAV vond van de door ons voorgelegde virussen het grootste aantal en blonk vooral uit in het vinden van macrovirussen en virussen die in binaire niet-rechtstreeks-uitvoerbare bestanden verstopt zijn.



# Kaspersky Personal AntiVirus



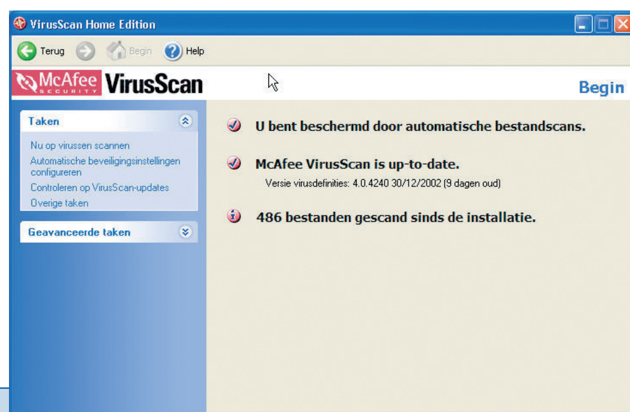
Het Russische AVP-pakket van Kaspersky Labs krijgt wereldwijd steeds meer aandacht. Zelfs het Finse F-Secure maakt gebruik van de antivirusinformatie van Kaspersky. We moeten eerlijk toegeven dat we onder de indruk zijn. Dit pakket doet zowat alles, maar het heeft geen zandbakfunctie voor het afschermen van allerlei kwaadaardig spul, zoals de eSafe Desktop. De preventie bestaat uit het in de achtergrond uitvoeren van scans en een paar basismaatregelen. De detectie is heel erg goed en vecht in onze testen meestal nek-aan-nek met die van F-Secure. We zien AVP wel zitten omdat het voor zowat elk besturingssysteem te vinden is en er allerlei andere beveiligingsmaatregelen te verkrijgen zijn bij de Benelux-leverancier ThunderStore. AVP kost heel wat minder dan de concurrentie (F-Secure is zelfs het duurst van allemaal). Van AVP kan je een aantal verschillende versies krijgen: een Lite, een Personal en een Personal Pro versie. De verschillen daartussen hebben te maken met wat je ermee kan beschermen en wat het pakket nog meer kan. Hoe meer het kan, hoe meer het kost – maar dat zal je wel niet verbazen.






## NAI McAfee VirusScan

De nieuwste antivirustelg van Network Associates is McAfee versie 7. Daar kan je een demoversie van downloaden, maar schrik niet: die is maar liefst 36 MB groot! Bij NAI vond men het niet nodig je daarvoor te waarschuwen op hun website: ze denken blijkbaar dat iedereen een breedbandaansluiting heeft... Behalve een virusscanner zit hier ook nog een back-upprogramma met geïntegreerde virusbescherming en een persoonlijke firewall bij. Zoals vanouds heten de belangrijkste antiviruselementen VirusScan (de eigenlijke detector) en VShield (achtergrondpreventie). Al die losse onderdelen worden allemaal keurig samen geïnstalleerd en je merkt er eigenlijk weinig van dat dat oorspronkelijk allemaal aparte software was. Bovenop al deze deelsoftware zit VConsole, een bedieningsconsole voor Windows die een soort van takenbeheer voorstelt. Net als bij FSAV en andere scanners in deze test configureer je onmiddellijk of later uit te voeren taken. NAI brengt minstens eenmaal per maand een nieuwe versie van de virusdatabase uit. Je kan die mits een wachtwoord van hun website halen of een abonnement afsluiten om je die per post te laten toezenden. Het automatisch aftasten van materiaal dat van het internet komt, is keurig voorzien en alle bewaaracties worden sowieso gecontroleerd via VShield.



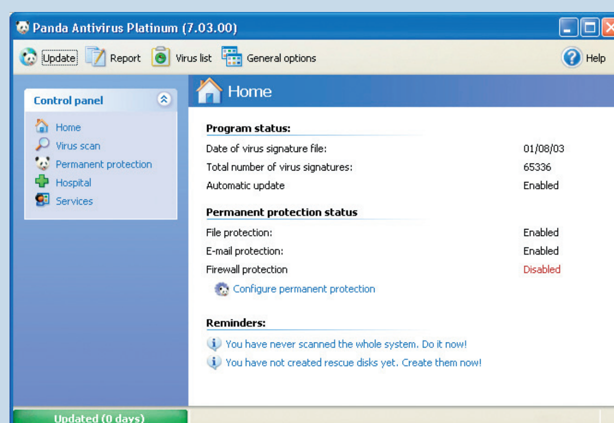




## Panda AntiVirus Platinum

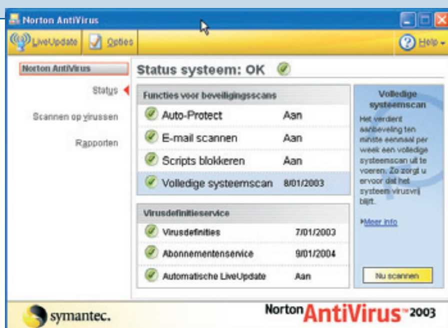



Panda Software is van Spaanse afkomst en beschikt over verschillende antivirusproducten, maar wij bekijken alleen de versie voor alleenstaand desktopgebruik. Qua mogelijkheden en gebruiksgemak lijkt het erg op de vooral Amerikaanse concurrentie. In de nieuwe Platinum-variant heeft Panda het gebruiksgemak echter naar een hoger niveau getild en dat merk je. Overigens bestaat er ook nog een goedkopere Titanium-versie voor thuisgebruikers, maar die heeft Panda niet opgestuurd: wel de Platinum voor SOHO-gebruikers. Wat het Panda-pakket er echt met kop en schouders uit doet springen is het niveau van de ondersteuning. Panda Software brengt dagelijks een update van de virusdatabase uit en ook de software zelf wordt zeer regelmatig bijgewerkt. Al deze updates kunnen gratis van het internet gehaald worden, mits je je registratiekaart instuurt, want dan pas krijg je het wachtwoord dat je daarvoor nodig hebt. Heel interessant: Panda verkondigt dat als jij een door hun software niet herkend virus tegenkomt, je hen mag contacteren en zij garanderen dan binnen de vierentwintig uur een nieuwe versie van de antivirussoftware die dat virus wél kent en kan onderscheppen. We hebben dat bij een vorige test eens uitgeprobeerd: we stuurden zes van de bestanden die hun scanner niet detecteerde naar Panda Software om te kijken wat zij ermee zouden doen. De volgende dag kregen we een nieuwe versie van de virusinformatiedatabase die de zes door ons doorgegeven virussen niet alleen herkende maar specifiek bij naam noemde. Dat laatste toont ons dat men bij Panda serieus onderzoek gedaan heeft naar de nieuwe virussen en niet gewoon klakkeloos een paar nieuwe signaturen in de database heeft gepropt.




### VAKTAAL

**Firewall:** Een veiligheidsvoorziening die de gegevenuitwisseling in het oog houdt. Wie zich op het internet begeeft, kan zich op die manier beschermen tegen personen die zonder toestemming zijn systeem binnendringen.




# Symantec Norton AntiVirus 2003

Net zoals bij veel concurrenten is de centrale interface van Norton AntiVirus een soort van takenbeheer. Het geheel is erg gebruiksvriendelijk en we vinden het hele bedieningssysteem een voorbeeld voor alle andere producenten. Zo moet het! De LiveUpdate-knop is ook nog steeds een voorbeeld voor alle andere softwareproducenten en heus niet alleen die van antivirussoftware. Overigens kan je met LiveUpdate alle producten van Symantec updaten, niet alleen het antivirusprogramma. Inzake preventie controleert Norton AntiVirus alle wijzigingsoperaties op je harde schijf. Alles wat niet is zoals het hoort – met name als iets probeert bestanden te wijzigen of

Meer informatie over deze antivirusprogramma's vind je op [ www.clickxmagazine.be ]





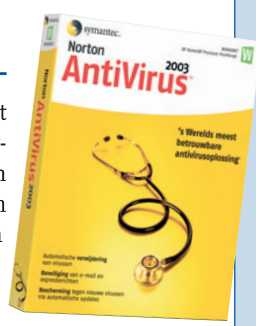




| MERK PRODUCTNAAM | | ESAFE DESKTOP | F-SECURE ANTIVIRUS | KASPERSKY PERSONAL ANTIVIRUS | NAI MCAFEE VIRUSSCAN | PANDA ANTIVIRUS PLATINUM | SYMANTEC NORTON ANTIVIRUS 2003 |
|---|---|---|---|---|---|---|---|
| Website merk | | www.esafe-desktop.com | www.f-secure.com | www.kaspersky.com | www.mcafee.com | www.panda-software.com | www.symantec.com |
| COMMERCIËLE INFO BELGIË | | | | | | | |
| Adviesprijs | | € 82 | € 97,59 | € 32 | € 47,57 | € 69,95 | € 49,99 |
| Leverancier | | Microcraft | Data Rescue | Infomaco | Data Alert | Panda Software NV | Symantec Belgium |
| Telefoonnummer | | 019/63.22.92 | 04/344.65.10 | 02/732.40.20 | 03/830.77.77 | 02/756.08.80 | 02/531.11.40 |
| Website | | www.micro-craft.be | www.data-rescue.be | www.ifomaco.com | www.data-alert.be | www.panda-software.be | www.symantec.com/region/nl/corporate/contact.html |
| PRODUCTKENMERKEN | | | | | | | |
| Evaluatieversie downloadbaar? | | Ja | Ja | Ja | Ja | Ja | Neen |
| Bescherming tegen infecties vanaf het internet? | | Ja (totale blokkade) | Ja | Ja | Ja | Ja | Ja |
| Gratis software-updates | | Ja | Ja | Ja (alleen met wachtwoord of registratie) | Ja (alleen met wachtwoord of registratie) | Ja (alleen met wachtwoord of registratie) | Ja |
| Gratis virusdatabase update via internet? | | Ja | Ja | Ja (alleen met wachtwoord of registratie) | Ja (alleen met wachtwoord of registratie) | Ja (alleen met wachtwoord of registratie) | Ja |
| Uitvoering virusdatabase update | | Met één knop | Automatisch | Automatisch | Automatisch | Automatisch | Automatisch |
| Preventiemaatregelen tegen infecties? | | Ja (beveiligde omgeving) | Ja | Ja | Ja | Ja | Ja |
| Virusverwijdering? | | Ja | Ja | Ja | Ja | Ja | Ja |
| Gepland automatisch starten van detectie? | | Ja | Ja | Ja | Ja | Ja | Ja |
| Aanmaak noodstartdiskettte? | | Ja | Ja | Ja | Ja | Ja | Ja |
| Persoonlijke firewall? | | Ja | Nee | Nee | Nee | Ja | Nee |
| Standaardduur ondersteuning en dienstverlening na aankoop? | | 1 jaar | 1 jaar | 1 jaar | 1 jaar | Onbeperkt | 1 jaar |
| Ondersteunde besturingssystemen (1) | | W9x, WNT+ | W9x, WNT+, W3x, DOS, OS2, Linux | W9x, WNT+, DOS, OS2, Linux, PocketPC, PalmOS | W9x, WNT+, W3x, DOS, Mac | W9x, WNT+, W3x, DOS, OS2 | W9x, WNT+, W3x, DOS, OS2, Mac |
| SCOREBEREKENING | WEGING | | | | | | |
| Functionaliteitsscore | 15% | 92 | 72 | 70 | 66 | 74 | 62 |
| Score op detectietest | 40% | 83 | 89 | 90 | 87 | 85 | 86 |
| Relatief schoonmaaksucces (t.o.v. detectieresultaat) | 35% | 0 | 80 | 79 | 72 | 78 | 57 |
| Absoluut schoonmaaksucces (t.o.v. hele viruscollectie) | 10% | 0 | 71 | 70 | 63 | 68 | 51 |
| Prestatiescore | 70% | 47 | 82 | 81 | 76 | 79 | 69 |
| Prijsscore (2) | 30% | 37 | 31 | 95 | 64 | 43 | 61 |
| PRIJS/PRESTATIESCORE | | 44 | 67 | 85 | 72 | 68 | 67 |

(1) W3x = Windows 3.1x & Windows for Workgroups 3.1x / W9x = Windows 95 SP2/98/98SE/Me / WNT+ = Windows NT4+/2000/XP
(2) Ideale prijs= € 25

te wissen waar dat niet zou mogen – blokkeert hij en geeft dan een waarschuwingsvenster. Norton AntiVirus blijkt niet zo goed in het repareren van besmette bestanden. Zorg dus altijd voor een gegarandeerd virusvrije back-up van je systeem als je dit product gebruikt, want je kan niet echt vertrouwen op de schoonmaakfaciliteiten.




## CONCLUSIE

ESafe Desktop is helaas niet langer gratis en dingt vanwege de bijzonder slechte detectie en schoonmaak niet mee naar een plaats op het ereschavot in onze test, maar we vonden dat het toch een aanbeveling verdient vanwege de fantastische totaalbescherming met het zandbaksysteem. We begrijpen nog steeds niet waarom andere antivirussoftwareproducenten zoiets niet inbouwen. De allerbeste scanner krijg je met F-Secure AntiVirus en Kaspersky Personal AntiVirus. De eerste is wel ruim drie keer zo duur. Vandaar dat Kaspersky Personal AntiVirus ons favoriet programma is.

## DE TEST

We onderzochten zes antivirusproducten. We hebben zelf een viruscollectie samengesteld van virussen die al ooit in onze contreien voorkwamen, of toch zoveel mogelijk. In totaal zitten er 18.741 virussen in onze collectie. Daarvan zijn de overgrote meerderheid van het COM-type (14.727 stuks): dit zijn niet de nieuwste maar wel nog steeds heel veel voorkomende virussen. Voorts hebben we 3.730 *exe*-bestanden met een virus aan boord en daar zitten wel nieuwe bij, onder meer beestjes zoals Nimda en het beruchte CIH-virus. Macrovirussen zijn natuurlijk ook belangrijk. Er zijn er duizenden, maar je kan ze onderverdelen in enkele tientallen hoofdgroepen. Wij hebben uit elke hoofdgroep één of meer macrovirussen gekozen met in totaal zo'n 269 verschillende macrovirussen. Dat zijn niet alleen Office-macro's, maar ook VB-scripts en dergelijke. Om het wat vollediger te maken hebben we ook nog vijftien bestanden met niet door de gebruiker uitvoerbare binaire bestanden (zoals OBJ- en DLL-bestanden, VXD-drivers voor Windows, startsectordata enzovoort). We noteerden hoeveel virussen door elk product herkend werden van elke soort en drukten het totaal uit als een percentage. Helaas bleek geen enkele scanner in staat ze allemaal te herkennen, zelfs de meest recente niet.

— Johan Zwiekhorst —

## VAKTAAL

**EXE:** Afkorting van Executable file, dat is een uitvoerbaar bestand of een programma.